New Steganography System Based on Huffman Coding and Fibonacci Decomposition

Fadheela Sabri Abu-Almash
Ministry of Higher Education and Scientific Research/
Scholarships and Cultural Relations Directorate
fofo200772@yahoo.com

Received in:23/July/2017, Accepted in: 12/December/2017

Abstract

Hiding secret information in the image is a challenging and painstaking task in computer security and steganography system. Certainly, the absolute intricacy of attacks to security system makes it more attractive.in this research on steganography system involving information hiding, Huffman codding used to compress the secret code before embedding which provide high capacity and some security. Fibonacci decomposition used to represent the pixels in the cover image, which increase the robustness of the system. One byte used for mapping all the pixels properties. This makes the PSNR of the system higher due to random distribution of embedded bits. Finally, three kinds of evaluation are applied such as PSNR, chi-square attack, and HVS attack.

Keywords: steganography, Huffman coding, embedding secret message, Fibonacci decomposition.

Introduction

Historically, design of any steganography system for digital images has heavily based on heuristic principles. Such steganography system aims to deal with cost of the pixels so the change will be in the relevant area of insignificant important and invisible to the human eye [1]. Steganography involves communicating secret message or information in an appropriate carrier such as video, audio, and image files. Each carrier has its own pros and cons, for video high payload capacity can embed but it is very sensitive against attack, same as audio media has less security when compared with image hosting media. The main goal here is to conceal enough information in suitable secure media, by considering image to carry the secret information gain worthiness to briefness the security of the system [2]. Steganography most of the time is defined as the art and science of hiding communication; hiding secret text message in hosting media like image called steganography. Two main techniques are used to hide secret data in image, spatial domain that is used pixel value and transform domain such as Discrete Transform Wavelet (DWT) and Discrete Cosine Transform (DCT) [3]. With our system, we consider spatial domain with pixel information, the best and simplest method to embed the secret bits directly in to the Least Significant Bit (LSB) in this plane hidden data cannot sense by human naked eyes due to the changing amplitude that occurred in pixel value which is too small [4]. For cover image, that hosting the secret message consists of 8-bitpalnes the most important one used for embedding is bitplane (1) and changing its value is little importance if compared with other bits. Fibonacci decomposition consists of 12-bitplanes that always used to increase the robustness of the steganography system [5]. In order to evaluate the system tree main requirements should be considered [6]: **Security** the main reason to hide the secret is to keep it secure as possible so no one even can feel if there is a secret message in image or not. Capacity it is useful to embed high payload secret message through one image so enough information will transmit to other party. Finally, **Robustness** which means the ability of the system to stop against any change of course under the same level of security and capacity.

Related Work

In last decade, many techniques produced by researchers most of them focusing on embedding methods and how to insert secret message into the cover image [7, 8 & 9]. Information hiding are classified into four categories, which are covert channel, steganography, anonymity, and copyright marking [10] and sub classification occur to the steganography into special and transform domains, each with its properties. Dimple A. and Amit D. explained what is the tools used in steganography and the format available [11] the most common data formats used are .txt, .bmp, .doc, .mp3, .jpeg and .avi etc. such steganography system used text message sending by image carrier for more robustness. Same researchers explored all the embedded method such as LSB, Random Pixel Embedding (RPE), Color Component (CC), Gray Level Modification (GLM) and Edge base Embedding (EBE) etc. Actually, the best method used to embed the secret into image is LSB [12] because it is easy and simple to use. Virtual bitplanes of Fibonacci decomposition used by Rakesh N. to embed the secret message [13] to increase the robustness of steganography system, he used bitplane (1) and bitplane (2) to increase the capacity by taking advantage of 12 bitplane of Fibonacci. Because of facility provided by Fibonacci many researchers used this technique [14 & 5]. The evaluation criteria for image steganography always-used Peak Signal-to-Noise Ratio (PSNR) refers to an expression for the ratio between the power value of signal and the power of noise that distorting the image quality and describe it in logarithmic scale. Choosing pixels from the image need special strategy for proposed system two strategies used knight tour and random generator. Knight tour is famous technique used to select block within the image [16], many systems used knight tour in steganography due to this technique which has

several advantages such as no replication of the same block number and difficult to predict the next block for security reason.

Sedighi V., et al in 2016 [17] proposed steganography system obtained state-of-the-art performance based on properly cover image estimator. They used closed-form expression for detectability within their method and consider empirical steganalysis detector as classifier.

Al-Dmour, H., et al in 2016[18] New algorithm suggested by embedding secret message in the sharp edge of cover image due to embedding in such location cause less degradation to the image quality. So that set pixels used to embed are not different from sharp and smooth area, because of that can protect the image from Human Visual System (HVS) attack that is less sensitive of changing in such area.

Sun, S. in 2016 [19] found new technique to embed the secret message into cover image using Canny edge detector and 2^K correction, this for security reason, and to enhance the payload capacity Huffman coding was used. He randomizes the pixels of edge detected to increase the security and 2^K achieved for better imperceptibility in stego image.

Akhtar, N. in 2016 [13] used LSB substitution by inverting bits before embedding to cover image to enhance the PSNR of stego image so the changing will occur on certain pixels not all for security reason.

Data Hiding Domain and Protocol

Data hiding technique can be classified into two groups: image domain and transform domain; image domain (also known as spatial domain) techniques embed secret message in the pixel intensity directly, and the transform domain (also known as frequency domain) secret message is embedded after transforming an image. Most of the images format used in secret embedding (steganography) is lossless and the technique always based on image format. Inserting message consider in less significant area which is containing of less important data such as LSB. That embed the data in this place cannot recognize by naked eyes. Therefore, the hosted secret may be able to be image, text, video or protocol as shown in figure (1).

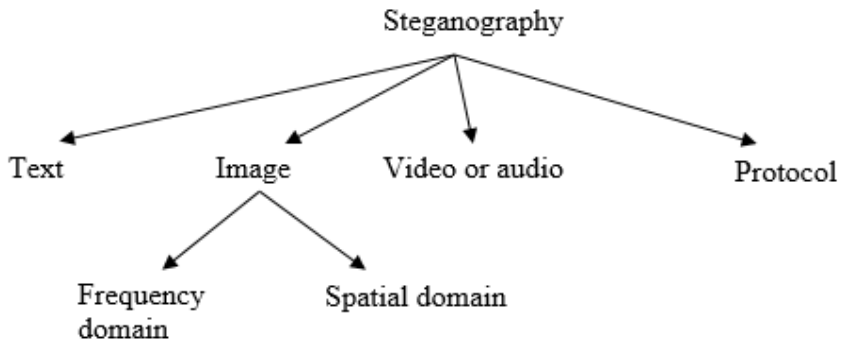

Figure (1): Image domain

Fibonacci decomposition is used to convert the coding of pixels data from binary into other formats called Fibonacci decomposition. first, we convert the physical 8-bitplanes image into logical 12-bitplanes Fibonacci decomposition using the following procedure:

```
publicint fibonacci(int x) {
        if (x==1)       return 1;
        else if (x==2)  return 1;
        else { return fibonacci(x-1) + fibonacci(x-2) }
```

In our case, the decimal number of the pixels changes directly to Fibonacci decomposition before doing any process on it. Hiding information inside the cover image when consider Fibonacci decomposition the data will become part of the image [20]. With proposed method, we translate something readable to unreadable media to secure the message that is mean just hidden data from plain view. To summarize how Fibonacci decomposition dose work and the sequence chain derived figure (2) illustrate the mechanism of this procedure:

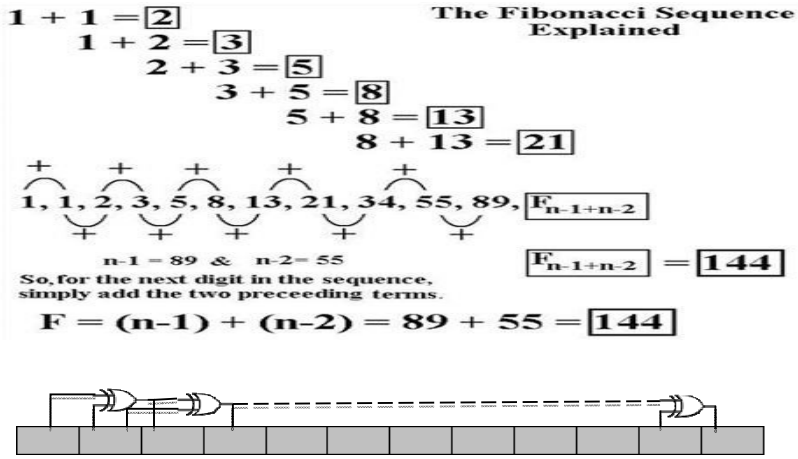

Figure (2): mechanism of Fibonacci sequence [20]

Proposed Method

For any steganography system there are four certain stages, these stages run sequentially and the most important stage is embedding stage which reflects the power of the algorithm. In proposed method, we deal with two stages which are preparing and embedding stages. In general, the main framework illustrates in figure (3).

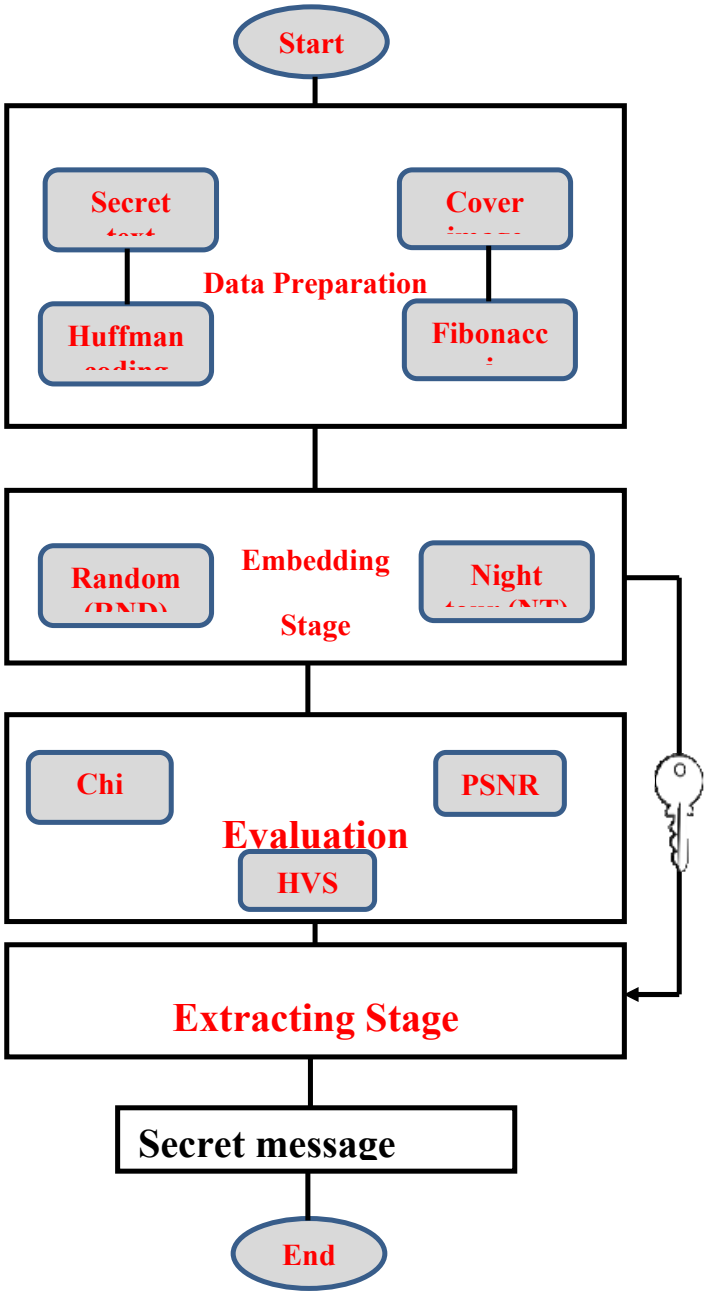

Figure (3): General framework of proposed method

The Huffman technique is useful to compress the secret message so that this procedure increases the capacity of message data and makes it more robust. This technique allows us to reduce the size of large secret message as such we embed large amount of data in one cover image, this is very important concept in term of data management and transfer protocol. Simple algorithm is shown in figure (4).

Input: Array *f[1...n]* of numerical frequencies or probabilities
Output: Binary coding tree with *n* leaves that has minimum expected code length for *f*.
huffman(*f [1...n]*)
T = empty binary tree
Q = priority queue of pairs (*i, f[i]), i = 1...n*, with f as comparison key
Foreach*k = 1...n − 1*
i= extractMin(*Q*)
j = extractMin(*Q*)
f[n + k] = f[i] + f[j]
insertNode*(T, n + k)* with children *i, j*
insertRear*(Q,(n + k, f[n + k]))*
Return*T*

Figure (4) Huffman algorithm

For image preparation, Fibonacci decomposition algorithm is used to deal with new decomposition of pixels data before embedding.

Embedding Method

Cover image consists of 8 x 8 blocks each with 64 x 64 pixels, the first block is chosen randomly to be the first point to apply knight tour algorithm. Then 63 blocks choosing will depend on knight tour algorithm movement. then the secret message embedding sequentially for each block according to its position in the sequence of movement in knight tour algorithm as shown in figure (5).

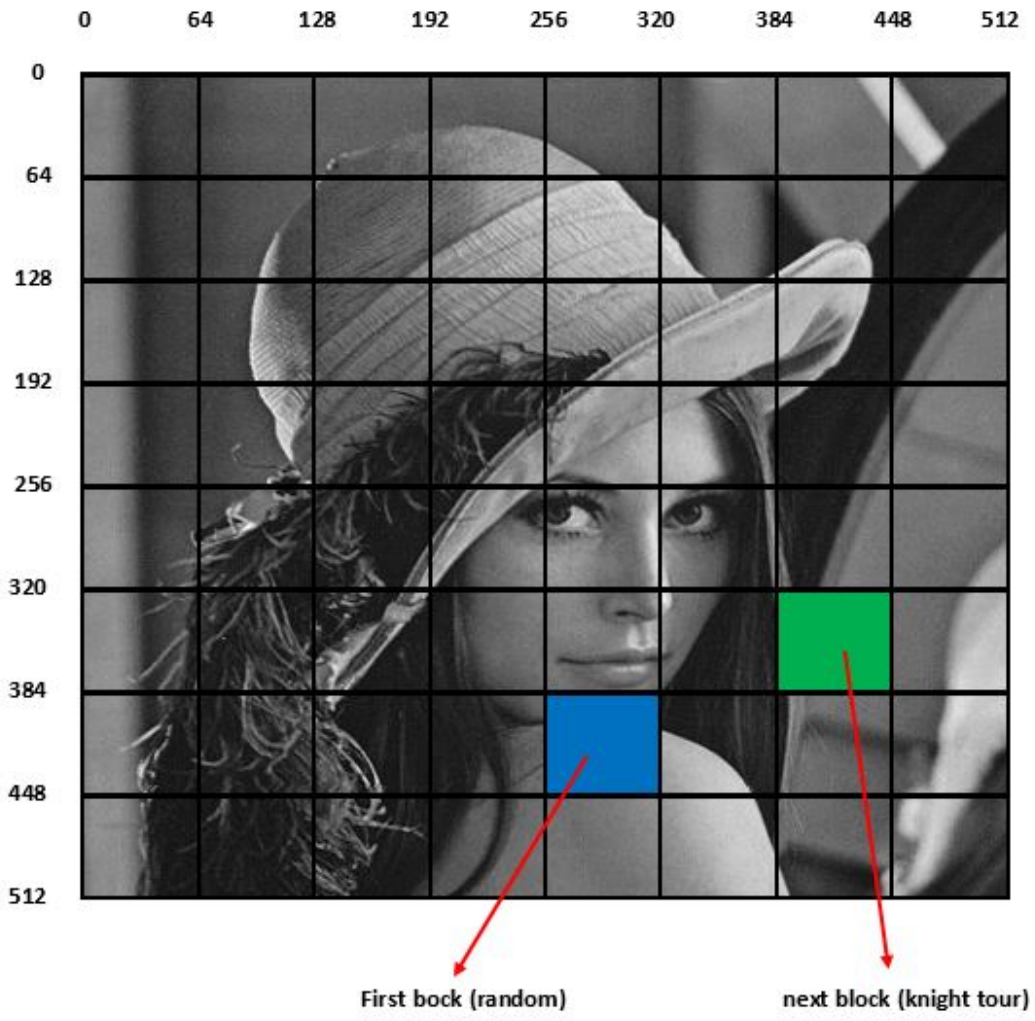

Figure (5): the first random block and next block

Then the embedding for pixels will embed sequentially for each pixel in block 64 x 64 after decomposing pixel from 8 bitplane to 12 bitplaine using Fibonacci sequence, using of knight tour strategy increase the security of the system [16], that reveal the benefits of knight tour algorithm with system embedding. Knight tour stage produce block of 8 x 8 pixels all these blocks are stored in KNvector.

Extracting Stage

The principle of steganography is to hide and send messages from one side (sender) into other side (receiver) via trusted media such image. With embedding the message will hide in the image using certain key which consists of the initial data for embedding, this data will send to the receiver side to use for extract the message from the image and finding the secret message as shown in figure (6).

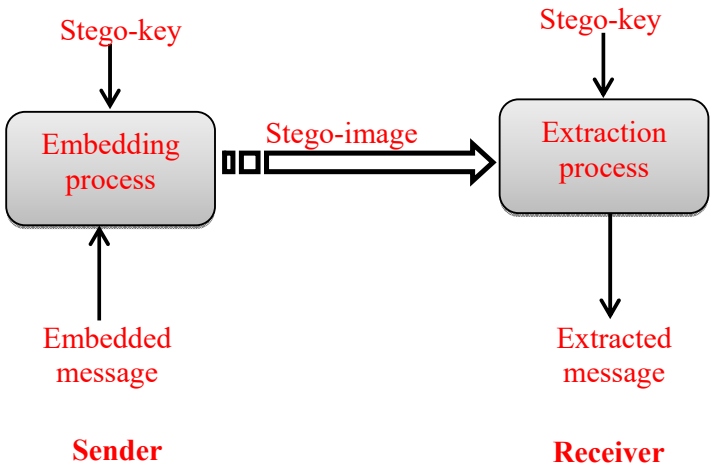

Figure (6): Steganography principles

Results and Discussion

Two important factors affecting the results on steganography system are the payload capacity that means how much secret message embedded to cover image, and the properties of the image such as dimensions, place of embedding … etc. However, PSNR is used to measure the quality of image after embedding and is defined as:

$$PSNR = 10.log_{10}(\frac{MAX_1^2}{MSE})$$

Where $MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$ and MAX ,is the maximum possible pixel value of the image; m , n are the dimensions of the image; I, K are original and noisy pixel.
The results of PSNR proved the worthiness of the proposed system as shown in figure (5).

Payload (Bytes)	Embedding (%)	PSNR (dB)		
		Fibonacci	Simple LSB	Proposed Method
16384	6.25	66.3536	62.2016	72.9154
32768	12.5	64.6589	61.2252	66.6366
49152	18.75	60.8680	59.7573	61.1637
65536	25	52.5675	50.8397	54.9036

(a) Lenaimage

Payload (Bytes)	Embedding (%)	PSNR (dB)		
		Fibonacci	Simple LSB	Proposed Method
16384	6.25	67.2556	62.9926	72.6584
32768	12.5	65.1119	62.6956	67.6986
49152	18.75	61.333	60.9683	63.0137
65536	25	53.3635	51.2268	56.8996

(b) Peppers image

Payload (Bytes)	Embedding (%)	PSNR (dB)		
		Fibonacci	Simple LSB	Proposed Method
16384	6.25	67.6532	61.8966	71.9965
32768	12.5	65.1219	61.0122	67.2346
49152	18.75	61.1003	58.7653	60.9625
65536	25	53.2055	49.3546	55.1394

(c) Baboonimage

Payload (Bytes)	Embedding (%)	PSNR (dB)		
		Fibonacci	Simple LSB	Proposed Method
16384	6.25	68.8421	60.2365	72.4658
32768	12.5	65.9859	60.2649	65.8564
49152	18.75	62.6954	56.9863	58.6525
65536	25	53.9821	50.2399	54.0215

(d) Cameramanimage

Figure (7): PSNR of proposed system

Different payload of secret message applied to show the relation between payload and PSNR where payload become less the distortion in the image will become less due to less pixels

affected by changing, on the contrary high payload will increase the distortion of the image then PSNR reduced.
The result stego image of proposed system cannot recognize by naked eyes but the system can have evaluated them by using the formula of PSNR as illustrated in figure (8).

Figure (8): Original Lena image before and after embedding with three methods

Images in figure (10) used **65536 bytes** payload capacity embedded to the methods of course high capacity will affect until certain amount then can easy recognize by the system and maybe by human eyes.
Other evaluation factor used here is Human Visual System (HVS) attack this kind of attack based on arrangement of the pixels in the stego image and will show if there is any particular embedding to the pixels or some arrange of them. For the reason HVS attack is used as shown in figure (9).

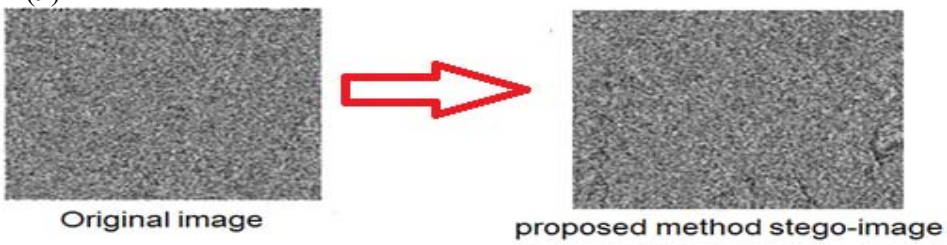

Figure (9) HVS attack for Lena image before and after embedding by three methods

Chi-square attach considers other evaluation factor used with proposed method. The idea of the statistical attack is to compare the theoretically expected frequency distribution in steganography with some sample distribution observed in the possibly changed carrier medium. Figure (10) shows the chi-square (X^2) attack for cameraman gray dataset. Y axis shows the probability of embedding the data in image as we can see the original image 20% of image indicates there is a data embedded inside it. With stego image produced from proposed method we reach approximately the same percentage of original image and this is the purpose of steganography algorithm.

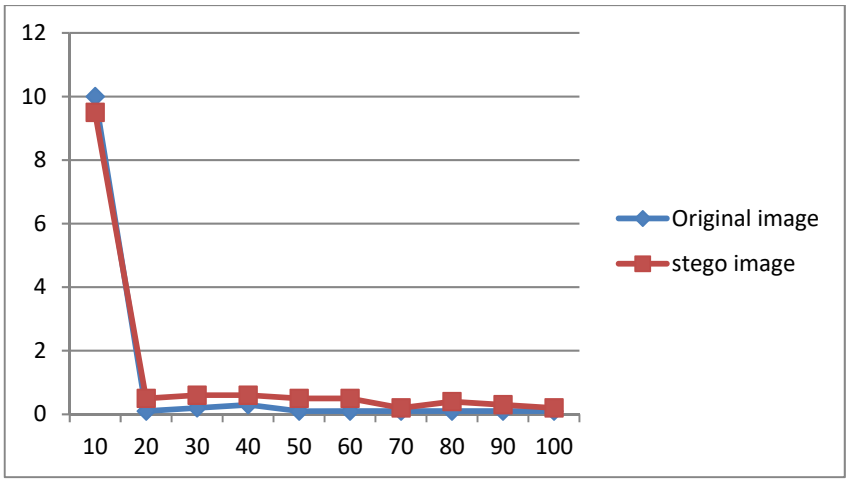

Figure (10): Chi-square attacks for cameraman dataset image

To evaluate how good proposed method compares with previous methods in literature we benchmark our results by embed 6.25% secret message payload in order to be equally criteria when compare as shown in figure (11). We can clearly see that our system can reach PSNR about (74.32) while other method is less than (70) due to checking bits to embed if the secret message is similar to bits in cove image with probability of changing or not change according to how many bits inverted in this procedure. This benchmarking for the cameraman gray image dataset with embedding 16384 bytes of secret message. Actually, this considers the higher PSNR because of payload capacity is considered too small, and the relation between capacity and PSNR is inversely related. That means high capacity lead to low PSNR and vice versa.

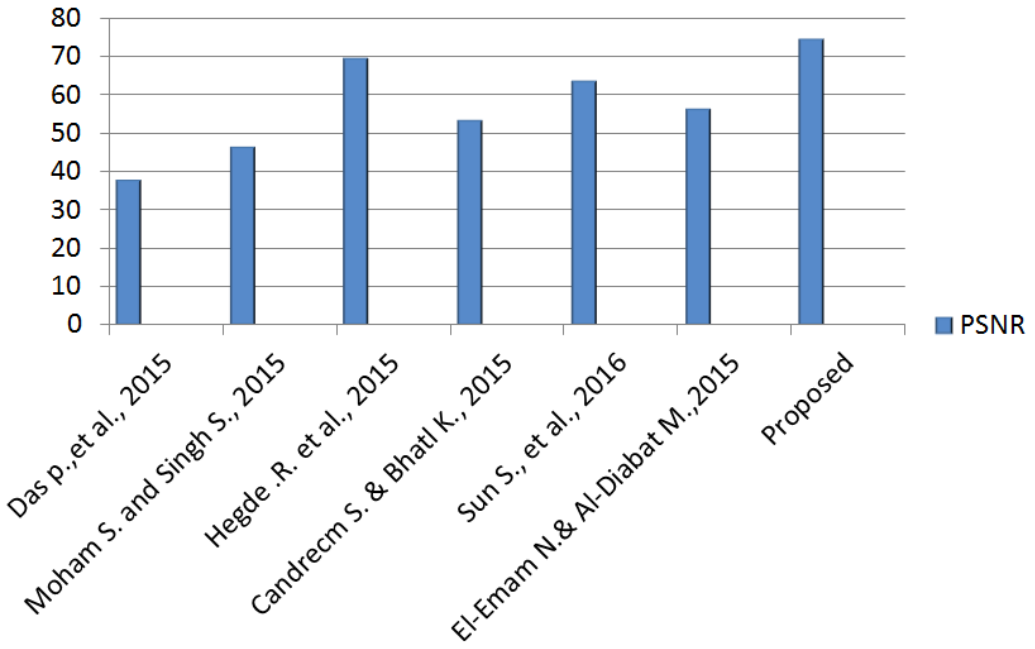

Figure (11): Benchmarking proposed method with literature using 6.25% embedding secret data.

Conclusion

The efficiency of the steganography system is by embedding method, and using Fibonacci increase the robustness of the system. Huffman encoding is used to increase the capacity of the steganography system. Reducing the bits is changed by insertion of secret message which makes the system strong against attacks; with proposed method we try to avoid embed secret data directly (by using two random algorithms) to the cover image we distribute over the image and changing bitplane into Fibonacci decomposition. using of compression algorithm in steganography system increase the capacity but still need to maintain the PSNR (image distortion) so proposed embedding method used compering with existing method there is no balancing between amount of data embedded and embedding strategy. Because of this proposed system got occasion results.

References

[1] V. Sedigh; R. Cogranne. and J. Fridrich, "Content-Adaptive Steganography by Minimizing Statistical Detectability". Information Forensics and Security, IEEE Transactions on, 11(2), 221-234 2016.

[2] M.Safarpour and M.Charmi, "Capacity Enlargement Of The PVD Steganography Method Using The GLM Technique". arXiv preprint arXiv:1601.00299 2016.

[3] H. Al-Dmour; N. Ali and A. Al-Ani, A. "An Efficient Hybrid Steganography Method Based on Edge Adaptive and Tree Based Parity Check." In MultiMedia Modeling (. 1-12). Springer International Publishing.

[4] S.Bhatt, A.Ray; A. Ghosh and A. Ray," Image steganography and visible watermarking using LSB extraction technique.InIntelligent Systems and Control " (ISCO), 2015 IEEE 9th International Conference on (1-6). IEEE January ,2015.

[5] N. M.Deval,"Secure Steganography Algorithm Based on Cellular Automata using Fibonacci Representation and Reverse Circle Cipher Application for Steganography" 2015 .

[6] M. K. Vinaykumar, and B. N.Vaishakh, "Key Based Data Embedding Technique in Image Steganography" ,International Journal of Computer Applications (0975 – 8887) 2013.

[7] J. Gupta,"A Review on Steganography techniques and methods" 2015.

[8] V.Rabara,andA.Goswami," A Survey of Image Based Steganography" . INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND SCIENCES, *1*(2), 1-4 2015.

[9] B. M.Vikranth; M. H.Momin, S. M. Mohsin;S. Rimal, and S. R. Pandey, " A SURVEY OF IMAGE STEGANOGRAPHY" .In Journal of Emerging Technologies and Innovative Research . 2. 4 (April-2015). JETIR.

[10] F. R.Patel, and A.N.Cheeran," Performance Evaluation of Steganography and AES encryption based on different formats of the Image.Performance Evaluation", 4(5) 2015 .

[11] D.Anandpara, & AD. Kothari, " Working and Comparative Analysis of Various Spatial Based Image Steganography", Techniques. International Journal of Computer Applications, 113(12):1–5. (0975 – 8887) 2015.

[12] J.Fridrich,and M.Goljan, U.S. Patent No. RE40,477. Washington, DC: U.S. Patent and Trademark Office 2008.

[13] R.Nayak,"Steganography with BSS-RSA-LSB technique: A new approach to Steganography". IJSEAT, 3(5), 187-190 2015.

[14] Z. A. S. Rasheed, "Steganography Technique for Binary Text Image.International Journal of Science and Research", (IJSR) ISSN (Online), 2319-7064 2015.

[16] A.Bansal; S. K.Muttoo andV.Kumar, " Secure Data Hiding by Optimal Placement of Queen Along Closed Knight Tour". i-Manager's Journal on Information Technology, 4(3), 18 2015.
[17] V.Sedighi , R.Cogranne, & J.Fridrich "Content-Adaptive Steganography by Minimizing Statistical Detectability" . Information Forensics and Security, IEEE IEEE Transactions on Information Forensics and Security 11 (2), 221-234 2016
[18] H.Al-Dmour, and A. Al-Ani, "A steganography embedding method based on edge identification and XOR coding" . *Expert Systems with Applications*, *46*, 293-306 2016
[19] S.Sun, " A novel edge based image steganography with 2 k correction and Huffman encoding". Information Processing Letters, 116(2), 93-99 2016.
[20] C. Patsakis, and E. Fountas, "Extending Fibonacci LSB data hiding technique to more integer bases". In Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on (. 4,. 4-18). IEEE August,2010 .